INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on April 6, 2004 between the Examiner and Applicants' representatives William James and Clover Huang. The Office Action mailed on January 21, 2004 was discussed. Specifically, the rejection of claims 22-29 in light of Hu et al. (U.S. Patent No. 5,574,912), claims 35-38 in light of Bergman et al. (U.S. Patent No. 6,442,694), and claims 8-11 in light of Conklin et al. (U.S. Patent No. 5,991,881), were discussed. Differences between the references and what is claimed were discussed with the intent to place the claims in better condition for allowance or appeal. No agreement was reached with respect to the claims. The Applicants wish to thank the Examiner for his time and attention in this case.

REMARKS

Claims 22-25, 30, 39 and 40 have been canceled. Claims 1, 3, 8, 18, 26, 28-33 and 41-43 have been amended to clarify the subject matter regarded as the invention. Claims 1-21, 26-29, 31-38, and 41-43 remain pending.

The Examiner has required under 37 CFR 1.105 information to identify products and services embodying the disclosed subject matter of a simplified version of the instant invention referenced in Provisional U.S. Patent Application No. 60/151,531, p. 15. The inventors named in the present application are no longer employed by or otherwise associated with assignee Symantec Corporation, which is prosecuting the present case as the assignee of all rights in the inventions disclosed and claimed in the application and, as a result, the inventors themselves were not available to provide first hand the requested information. To the best of assignee's knowledge, the above-cited reference with respect to which the Examiner has requested information refers to the "DERBI" (Diagnosis, Explanation and Recovery from Computer Break-Ins) project at SRI International, concerning which information is available on SRI International's website at http://www.ai.sri.com/~derbi, representative pages of which are included in an Information Disclosure Statement filed concurrently herewith. Applicants note that the DERBI project is referenced in footnote 17 of the Durst article referenced in the above-cited provisional application and in paragraph 3 of the Office Action.

The Examiner states that the provisional applications upon which priority is claimed fail to provide adequate support for the claims of the present application under 35 U.S.C. 112. The application has been amended to delete the claim of priority to U.S. Patent Application No. 60/143,821. Applicants believe provisional U.S. Patent Application No. 60/151,531 provides adequate support for the claims. See, e.g., pages 7, 11, and 18. On page 7 (last two paragraphs), the problem of a high alarm rate leading to a delayed handling of alarms is described, and on page 11 (first two paragraphs), the specific problem of flooding an IDS with false alerts to prevent timely detection of a significant attack is described. On page 18 (paragraph above "Summary"), it is described how the processing of a collection of data may be reordered, and not necessarily performed in order, to ensure that all data is timely processed. Similarly, claim 1 describes a queuing process that reorders a collection of data for processing to address the problem of a flood of false or less significant alerts masking a more significant attack. It is therefore believed that the Applicant's claim for domestic priority under 35 USC 119(e) to provisional U.S. Patent Application No. 60/151,531 is proper.

The Examiner has requested a replacement copy of Paper No. 3, an IDS filed 13 November 2000. The Applicant does not know of any IDS's filed other than the Forms 1449 filed on 8 June 2001 and 13 November 2000 that were returned in this Office Action. Applicant suspects the Form 1449 filed 13 November 2000 may have been entered in duplicate in the Patent Office as both Paper No. 3 and Paper No. 5, as both have the same filing date.

The Examiner has indicated that the drawings are objected to as failing to comply with 37 CFR 1.84(g), 37 CFR 1.84(l), and 37 CFR 1.84(p)(1). It is believed that the attached formal drawings overcome the objections to the drawings.

The Examiner has objected to the abstract for not adequately encompassing the breadth of the disclosure. The abstract has been amended to overcome the Examiner's objections.

The Examiner has rejected claim 18 under 35 USC 112, second paragraph as being indefinite. Claim 18 has been amended to recite "a service identified as vulnerable to attack." It is believed that claim 18 as amended satisfies the requirements of 35 USC 112, second paragraph.

The Examiner has rejected claims 1-21, 26-29, 31-38, and 41-43 under 35 USC 103(a).

The rejections are respectfully traversed. The Office Action acknowledges on page 10, paragraph 16 that neither Conklin nor Knuth discloses the use of more than one queue as recited in claim 1 as amended. The Hu reference relied on in rejecting claim 22 describes placing processes in queues based on their security classifications. The queues are scheduled for processing in order of increasing security class. This lowers the potential of a covert channel giving unauthorized access to data. Hu is not concerned with and therefore does not address the problem of ensuring that data associated with a critical security event is timely selected for processing notwithstanding the prior receipt of numerous sets of less critical data, as recited in claim 1. Specifically, Hu does not teach placing each of a plurality of successive sets of data "in a selected one of a plurality of queues based at least in part on a queue selection algorithm by which sets of data associated with related security events are grouped into the same queue while sets of data associated with unrelated security events are spread across different queues; and processing the sets of data by: (1) selecting for processing a first set of data from a first queue; (2) selecting for processing a next set of data from a next queue in order that contains a set of data; and (3) repeating step (2) until no queue contains a set of data that has not yet been selected for processing; whereby a critical set of data associated with a critical security event is timely selected for processing even under circumstances in which numerous sets of data associated with a corresponding set of security events that are related to each other but not to the critical security event are received prior to the critical set of data being received," as recited in claim 1. As such, claim 1 is believed to be allowable.

Claims 2-21, 26-29, and 31-38 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claim 8 is believed to be allowable for the additional reason that the Conklin reference does not describe "sending via a trusted third party a handoff message comprising information concerning the data to an administrative domain other than the administrative domain in which the data was received," as recited in Claim 8 as amended. The amendment to claim 8 is supported in the application at page 34, line 22 (last line) to page 35, line 8. Therefore, claim 8 is believed to be allowable for this additional reason.

Claims 35-38 are believed to be allowable for the additional reason that Bergman does not teach tracking messages associated with an attack back to identify a point of attack at which messages associated with the attack are entering the network," as recited in claim 35. Bergman describes a distributed method of identifying the first node in a network to experience an attack. Each node that is attacked sends a message to other nodes indicating that it was attacked. Each node can then determine whether it is the first node attacked based on the messages it receives from other nodes. The node that is the first attacked then sends an alert. (Column 15, lines 19-25) In contrast, claims 35-38 describes an iterative method of identifying a source of an attack. The method includes tracking messages associated with an attack back to the point of attack. Starting with a first device, the ports are scanned for messages associated with the attack. A first port is identified as associated with the attack. If the port is not an external connection, the process moves on to a second device to which the first port is connected. As with the first device, the ports are scanned for messages associated with the attack, and a second port is identified as associated with the attack. Bergman does not describe such an iterative approach. Claims 35-38 are therefore believed to be allowable for this additional reason.

Claims 41 and 42 recite systems for carrying out the method of claim 1. Therefore, it is believed that claims 41 and 42 are also allowable.

Claim 43 recites program code for carrying out the method of claim 1. Therefore, it is believed that claim 43 is also allowable.

The Examiner has rejected claims 1, 20, and 41-43 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 6,647,400 to Moran in view of Knuth, "The Art of Computer Programming, Volume 1," 2nd Edition, 1973, pp. 234-238. The terminal disclaimer filed concurrently herewith is believed to overcome the double patenting rejection.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Clover Huang

Clover Huang
Registration No. 55,285
V 408-973-2594
F 408-973-2595

VAN PELT AND YI, LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014